104 – Signature Analysis

Team Information

Team Name: @ls0-ra@n

Results Email: [redacted]

Examination Time Frame: to

Instructions

Description: Examine the files in the **104_Signature_Analysis_Challenge2008** folder to determine which files are using the proper signature information and filename display and which are not. Report the full filename for mismatched files, a detailed explanation of your process (software or technique) used to examine and determine your results, and provide the corrected file.

Points will be awarded for each successfully identified signature mismatch and reasoning for your decision.

Total Weighted Points: 10 Total Points available per entry – Total 100 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

Question 104: Signature Analysis

The following command was run in cygwin on a Windows XP laptop from the 104_Signature_Analysis_Challenge2008 folder:

$ file * > ../Results/104/file_output.txt

The file command attempts to classify each argument passed, and the results are output to a file, providing the following:

245.JPG: JPEG image data, EXIF standard

249.JPG: JPEG image data, JFIF standard 1.01

255.JPG: JPEG image data, EXIF standard

AutoWire.bmp: PC bitmap data, Windows 3.x format, 601 x 440 x 8

Bluestar.gif: GIF image data, version 89a, 1002 x 635

CLOCK.MOV: Microsoft Cabinet archive data, 40411 bytes, 2 files

Chaff_Floral_1179.bmp: PC bitmap data, Windows 3.x format, 1024 x 768 x 8

Chaff_Landscape_158.gif: GIF image data, version 87a, 252 x 204

Chaff_Landscape_161.gif: GIF image data, version 89a, 200 x 132

DollL Sales Worldwide.html: JPEG image data, JFIF standard 1.01

SAILBOAT.JPG: MS Windows HtmlHelp Data

SYSTEM.1ST: Windows 95/98/ME registry file

SYSTEM.CB: ASCII text, with CRLF line terminators

Windows.wav: shell archive or script for antique kernel text

blank.jpg: ASCII English text, with CRLF line terminators

blue.bmp: ASCII English text, with CRLF line terminators

intro.mpeg: Zip archive data, at least v2.0 to extract

ipp_0004.asp: ASCII English text, with CRLF line terminators

pctools.zip: data

straightline.tif: ASCII English text, with CRLF line terminators

This tells us that the following signatures are correct:

245.JPG

249.JPG

255.JPG

AutoWire.bmp

Bluestar.gif

Chaff_Floral_1179.bmp

Chaff_Landscape_158.gif

Chaff_Landscape_161.gif

And also tells us how to correct the following signatures:

CLOCK.MOV	--> CLOCK.MOV.cab
DollL Sales Worldwide.html	--> DollL Sales Worldwide.html.jpg
intro.mpeg	--> intro.mpeg.zip
SAILBOAT.JPG	--> SAILBOAT.JPG.chm
SYSTEM.1ST	--> SYSTEM.1ST.reg

Leaving the following files to decipher:

SYSTEM.CB

Windows.wav

blank.jpg

blue.bmp

ipp_0004.asp

pctools.zip

straightline.tif

The following command was run in cygwin on a Windows XP laptop from the 104_Signature_Analysis_Challenge2008 folder:

$ strings pctools.zip

This command reveals numerous references to Verisign and Microsoft, combined with the binary nature of the file indicates it is a digital certificate. Comparing the output of strings with other certificate types, it was apparent that this was a p7b type certificate.

pctools.zip --> pctools.zip.p7b

Windows.wav is reported as archive or script text, implying it is safe to view. Visual inspection reveals the following:

Windows.wav --> inappropriately labeled, actually a .cnt file

Knowing that the rest of the files are simply ASCII text implies that they can be safely viewed. Visual inspection reveals the following:

blank.jpg --> inappropriately labeled, actually an asp page

blue.bmp --> inappropriately labeled, actually an asp page

ipp_0004.asp --> appropriately labeled as an asp page

straightline.tif--> inappropriately labeled, actually an asp page

SYSTEM.CB --> inappropriately labeled, actually an ini file

To summarize, the following files were using proper signature information:

245.JPG

249.JPG

255.JPG

AutoWire.bmp

Bluestar.gif

Chaff_Floral_1179.bmp

Chaff_Landscape_158.gif

Chaff_Landscape_161.gif

ipp_0004.asp

The following are the corrected file signatures:

blank.jpg.asp

blue.bmp.asp

CLOCK.MOV.cab

DollL Sales Worldwide.html.jpg

intro.mpeg.zip

pctools.zip.p7b

SAILBOAT.JPG.chm

straightline.tif.asp

SYSTEM.CB.ini

SYSTEM.1ST.reg

Windows.wav.cnt